PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-236147
(43)Date of publication of application : 23.08.1994

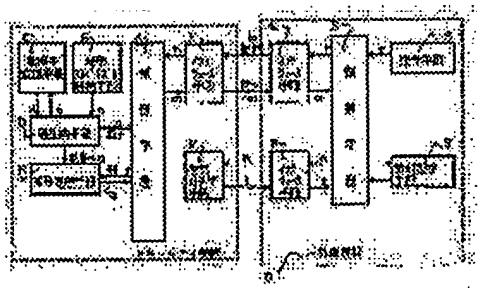
(51)Int.Cl. G09C 1/00
G06K 17/00

(21)Application number : 05-044432
(22)Date of filing : 10.02.1993

(71)Applicant : PANPUKIN HOUSE:KK
(72)Inventor : IMAI HIDEKI

(54) SECURITY DEVICE

(57)Abstract:
PURPOSE: To prevent to write in and read out illegally information of magnetic stripes, while cryptographic processing is enabled without a previous arrangement and delivery of a cryptographic key by inputting an identifier of a specific entity and generating the cryptographic key by a key generating means.
CONSTITUTION: A control means A of this device takes out an identifier (a) of a partner entity out of indication information (b) inputted from an interface means N and sends it to a key generation means D. And a peculiar cryptographic key (e) being common with the partner entity is generated by operating an identifier (d) to which the identifier (a) is converted by an identifier exchanging means C and a secret algorithm (c) stored in a secret algorithm storing means B, and sent to a cryptographic processing means E. Also, information written in a magnetic stripe means M of this device is sent to the cryptographic processing means E of this device from an external device 0, ciphered by using the cryptographic key (e), made ciphered information (q), and returned to the external device 0 from the interface means N as a response (m).



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平6－236147

(43)公開日　平成6年(1994)8月23日

(51)Int.Cl.[5]	識別記号	庁内整理番号	FI	技術表示箇所
G09C 1/00		8837－5L		
G06K 17/00		T 7459－5L		

審査請求　未請求　請求項の数3　FD　（全 6 頁）

(21)出願番号　特願平5－44432

(22)出願日　平成5年(1993)2月10日

(71)出願人　393009356
株式会社パンプキンハウス
神奈川県厚木市飯山1620番地の1　アメニティヒル本厚木717

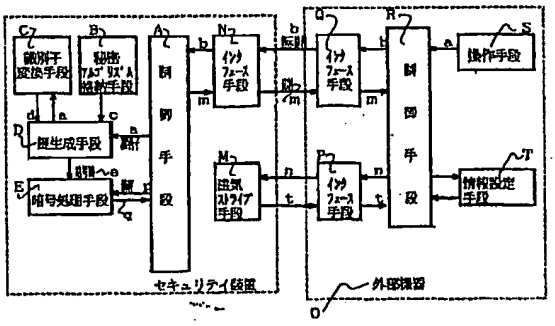
(72)発明者　今井　秀樹
神奈川県横浜市南区六ツ川3－76－3－J902

(54)【発明の名称】　セキュリテイ装置

(57)【要約】　（修正有）

【目的】　本発明は、任意に定めることのできる公開された相手エンテイテイの識別子を自分の秘密アルゴリズムに入力するだけで相手エンテイテイと自分に固有の暗号鍵を生成する鍵共有方式暗号システム（ＫＰＳ）による鍵生成手段を用いて暗号鍵を生成させ、この鍵を用いて磁気ストライプ上の情報を暗号化して記録及び／または読みだして復号することにより磁気ストライプ上のセキュリテイを確保するセキュリテイ装置を実現する。

【構成】　秘密アルゴリズムを格納する秘密アルゴリズム格納手段と、エンテイテイの識別子を変換する識別子変換手段と、識別子変換手段の出力と秘密アルゴリズム格納手段から暗号鍵を生成する鍵生成手段と、鍵生成手段で生成した暗号鍵を用いる暗号処理手段と磁気ストライプ手段で構成する。



1

【特許請求の範囲】

【請求項1】　各エンテイテイ（人、装置など）が公開の識別子を有し、センタ（管理者）が、センタだけが持つ特別なアルゴリズム（情報）とエンテイテイの識別子に一方向性でランダムな単射を行う識別子変換を施したものとを演算させてエンテイテイに固有な秘密アルゴリズム（情報）を生成し、これを格納する秘密アルゴリズム格納手段と、前記識別子変換手段と、任意のエンテイテイの識別子を前記識別子変換手段で変換したものと前記秘密アルゴリズムを演算させて自分と任意のエンテイテイに固有の暗号鍵（鍵）を生成させる鍵生成手段と、暗号処理手段と、磁気ストライプ手段を具備して、前記磁気ストライプ手段に記録される及び／または記録された情報を、前記鍵生成手段で生成した暗号鍵を用いて前記暗号処理手段で暗号化及び／または復号することを特徴とするセキュリテイ装置。

【請求項2】　複数の前記秘密アルゴリズム格納手段を有し、それらから任意の秘密アルゴリズムを用いて暗号鍵の生成を行うことを特徴とする請求項1のセキュリテイ装置。

【請求項3】　記憶手段をさらに具備したことを特徴とする請求項1及び請求項2のセキュリテイ装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、セキュリテイ装置に関する。

【0002】

【従来技術】情報の暗号化／復号を行う暗号装置がある。また、磁気ストライプを有するカードが普及している。

【0003】

【発明が解決しようとする問題点】キャッシュカード、クレジットカード、プリペイドカードなどが、磁気ストライプを有するカード（磁気ストライプカード）として普及しているが、磁気ストライプ上の情報は不正にコピーすることができ、情報保全上に問題がある。また、種々の情報を記録するＩＣカードなどがあるが、これには情報の漏洩などの問題がある。さらに、情報保全のため、暗号機能を内蔵させて情報の暗号化と復号を行う暗号装置が実現されているが、これには通信を行う当事者間で暗号鍵の打合わせが必要であり、さらにその鍵を安全に保管する為の管理が必要となる。

【0004】

【課題を解決する為の手段】本発明は、各エンテイテイ（人、装置など）が公開の識別子を有し、センタ（管理者）が、センタだけが持つ特別なアルゴリズム（情報）とエンテイテイの識別子に一方向性でランダムな単射を行う識別子変換を施したものとを演算させてエンテイテイに固有な秘密アルゴリズム（情報）を生成し、これを格納する秘密アルゴリズム格納手段と、前記識別子変換

2

手段と、任意のエンテイテイの識別子を入力するだけで暗号鍵を生成する鍵共有方式暗号システム（以下、ＫＰＳという）の理論を用いた鍵生成手段と、暗号処理手段と、磁気ストライプ手段を具備し、特定のエンテイテイの識別子を入力して前記識別子変換手段を施したものと前記秘密アルゴリズムとを演算させて暗号鍵（鍵）を生成させ、この鍵を用いて前記磁気ストライプの情報を前記暗号処理手段で暗号化して記録及び／または読み出して復号することにより、前記磁気ストライプの情報を不正に書込むことや読み出すことを防ぐセキュリテイ装置を実現する。

【0005】さらに、記憶手段を具備することにより格納する及び／または格納された情報を、前記鍵生成手段で生成した暗号鍵と前記暗号処理手段で暗号化及び／または復号してこれらの情報に対する不正な書込みや読み出しを防止することを可能としている。また、複数の秘密アルゴリズム格納手段を具備し、秘密アルゴリズムを複数内蔵してそれらから任意の１つを用いて暗号鍵生成を行うことにより、本発明によるセキュリテイ装置を複数のエンテイテイで共用することや、一人のエンテイテイが複数の識別子を持ちそれぞれの識別子に対応する秘密アルゴリズムを有することや、異なる複数のセンタのアルゴリズムで生成された複数の秘密アルゴリズムを持つことが可能なセキュリテイ装置を実現した。

【0006】

【実施例】図１は、本発明請求項１のセキュリテイ装置（以下、本装置という）の一実施例で、本装置とそれを用いる外部機器Ｏの構成例及びその動作を説明する図である。本装置は、制御手段Ａ、秘密アルゴリズム格納手段Ｂ、識別子変換手段Ｃ、秘密アルゴリズムと識別子変換手段Ｃの出力から暗号鍵を生成する鍵生成手段Ｄ、鍵生成手段Ｄで生成した暗号鍵を用いて情報の暗号化／復号を行う暗号処理手段Ｅ、磁気ストライプ手段Ｍ及び外部機器Ｇと情報の送受信を行うインタフェース手段Ｎで構成される。外部機器Ｏは、制御手段Ｒ、本装置のインタフェース手段Ｎを接続するインタフェース手段Ｑ、本装置の磁気ストライプ手段Ｍの情報を書込む又は読み出すためのインタフェース手段Ｐ、各種操作や情報入力を行う操作手段Ｓ、操作手段Ｓやインタフェース手段Ｐから入力された情報を設定する情報設定手段Ｔで構成される。ここで、制御手段Ａ、並びにＲ、暗号処理手段Ｅ、識別子変換手段Ｃ、鍵生成手段ＤはＣＰＵ、メモリ及びプログラム、秘密アルゴリズム格納手段Ｂはメモリで構成することができる。

【0007】本装置と外部機器Ｏを用いて、磁気ストライプの情報を暗号化して書込み、又は読み出して復号することにより不正な書込みや読み出しを防止する処理について図１により説明する。外部機器Ｏの操作手段Ｓから入力された相手エンテイテイ（人、装置）の識別子ａは、制御手段Ｒにより指示情報ｂとしてインタフェース

手段Qを経て本装置のインタフェース手段Nに送られる。本装置の制御手段Aは、インタフェース手段Nから入力された前記指示情報bより前記識別子aを取り出して鍵生成手段Dに送り、これを識別子変換手段Cで変換したdと秘密アルゴリズム格納手段Bに格納された秘密アルゴリズムcとを演算させて相手エンテイテイとの固有な暗号鍵eを生成させ，暗号処理手段Eに送る。また、本装置の磁気ストライプ手段Mに書込む情報は、外部機器Oから本装置の暗号処理手段Eに送られ前記暗号鍵eを用いて暗号化されて暗号化情報qとなり、インタフェース手段Nより応答mとして外部機器Oへ返される。外部機器Oの制御手段Rは、インタフェース手段Qで受信した前記応答mから暗号化情報qを取り出して本装置の磁気ストライプ手段Mへの書込みを行う。また、前記磁気ストライプ手段Mに書込まれた暗号化情報tは、インタフェース手段Pで読み出されて本装置の暗号処理手段Eに送られ前記暗号鍵eを用いて復号されて復号情報qとなり、インタフェース手段Nより応答mとして制御手段Rへ返される。

【0008】ここで、本発明が使用している打合せや第三者による暗号鍵（鍵）の配送を必要とせずに、自分と任意のエンテイテイに固有の鍵を生成するＫＰＳについて説明する。エンテイテイｉが、半固定的に用いるもので任意に定められる公開の識別子を有し、これを識別子Ｙｉとし、これに一方向性でランダムな単射を行う識別子変換Ｆを施したものをＺｉ（数式１）とする。センタだけが持つ特別なアルゴリズム（情報）Ｇと、前記Ｚｉとを演算させて、エンテイテイｉに固有な秘密アルゴリズム（情報）Ｘｉ（数式２）を生成する。

【数１】

【数２】エンテイテイｉは、自分の秘密アルゴリズムＸｉにエンテイテイｊの識別子Ｙｊを識別子変換したものＺｊを入力し、演算させて（数式３）、エンテイテイｊとの共通な暗号鍵ｋｉｊを生成させることができる。またエンテイテイｊの秘密アルゴリズムＸｊに、エンテイテイｉの識別子Ｙｉを識別子変換したＺｉを入力して演算し（数式４）、鍵ｋｊｉを生成させることができ、これが前記ｋｉｊに等しい（数式５）ので、エンテイテイｉが暗号鍵ｋｉｊで暗号化した内容は、エンテイテイｊに復号させることができる。

【数３】

【数４】

【数５】ＫＰＳの理論的な詳細ついては、文献１から文献５等に記述されている。

【0009】図２は、本発明請求項２の一実施例とその動作を示す図である。図中Ａ及びＣからＴ、ａからｑは図１と同じである。本発明請求項２のセキュリテイ装置は、複数の秘密アルゴリズム格納手段を示す秘密アルゴリズム格納手段ア（Ｂ１）、秘密アルゴリズム格納手段イ（Ｂ２）と、選択手段Ｕとをさらに具備している。暗

号鍵生成時に制御手段Ａからの制御情報ｒにより、選択手段Ｕは複数の秘密アルゴリズム格納手段から一つを選択して鍵生成手段Ｄに転送する。

【0010】図３は、本発明請求項３の一実施例とその動作を示す図である。図中ＡからＴ、ａからｑは図１と同じであり、さらに記憶手段Ｖを具備する。記憶手段Ｖの情報を、鍵生成手段Ｄで生成した暗号鍵ｅと暗号処理手段Ｅで暗号化して外部装置Ｏに送り、これを外部装置Ｏが磁気ストライプ手段Ｍに書込むことにより記憶手段Ｖの情報を不正な書込みや読み出しの困難な暗号情報として磁気ストライプ手段に記録すると共に、これを外部装置Ｏが読みだして本装置に送って復号させ、予め記憶手段Ｖに記憶した情報と照合させることなどができる。

【0011】

【発明の効果】本発明によるセキュリテイ装置は、任意のエンテイテイの識別子を入力するだけで暗号鍵を生成する鍵共有方式暗号システム（以下、ＫＰＳという）の理論を用いた鍵生成手段と、識別子変換手段と、秘密アルゴリズム格納手段を、暗号処理手段と磁気ストライプ手段を持った装置に内蔵させ、特定のエンテイテイの識別子を入力して前記鍵生成手段で暗号鍵（鍵）を生成させ、この鍵を用いて磁気ストライプの情報を前記暗号処理手段で暗号化して書込み、または読み出して復号することにより、磁気ストライプの情報を不正に書込むことや読み出すことを防ぐと共に暗号鍵の打合せや配送を不要として暗号処理を行うことを可能とした。

【0012】また、複数の秘密アルゴリズム格納手段をさらに具備し、秘密アルゴリズムを複数内蔵してそれらから任意の１つを選択することにより、複数のエンテイテイで共用するセキュリテイ装置や、一人のエンテイテイが複数の識別子を持ちそれぞれの識別子に対応する秘密アルゴリズムを有したセキュリテイ装置や、異なる複数のセンタのアルゴリズムで生成された複数の秘密アルゴリズムを内蔵してセンタのアルゴリズムの更新に対応することや、異なるセンタ間での共有鍵の生成が可能なセキュリテイ装置を実現する。さらに、記憶手段を具備してこれに格納する、または格納された情報を、前記暗号鍵生成手段で生成した暗号鍵と前記暗号処理手段により暗号化または復号することによりこれらの情報を不正に書込むことや読み出すことを防ぐと共に、これを磁気ストライプ手段に記録することにより、磁気ストライプ上の情報を不正にコピーして悪用することを防ぐことが可能となる。

【0013】クレジットカード、キャッシュカード、プリペイドカード等従来磁気ストライプカードで実現しているこれらの機能は、本装置をカードで実現してその一端に磁気ストライプ手段Ｍを設定することにより、従来の磁気ストライプ用機器で本装置を利用することができる。

【図面の簡単な説明】

5

【図１】本発明請求項１の一実施例とその動作を説明する図である。

【図２】本発明請求項２の一実施例とその動作を説明する図である。

【図３】本発明請求項３の一実施例とその動作を説明する図である。

【符号の説明】

A	制御手段
B	秘密アルゴリズム格納手段
B１	秘密アルゴリズム格納手段ア
B２	秘密アルゴリズム格納手段イ
C	識別子変換手段
D	鍵生成手段
E	暗号処理手段
M	磁気ストライプ手段
N	インタフェース手段
O	外部機器
P	インタフェース手段
Q	インタフェース手段
R	制御手段
S	操作手段
T	情報設定手段
U	選択手段
V	記憶手段
a	識別子
b	指示情報
c	秘密アルゴリズム情報
d	識別子変換された情報
e	暗号鍵
m	応答
n	書込み情報
t	読みだし情報
p	平文／暗号文情報
q	暗号化／復号情報
r	制御手段と選択手段間の制御情報

【数１】Ｚｉ＝Ｆ（Ｙｉ）

【数２】Ｘｉ＝Ｇ（Ｚｉ）

6

【数３】ｋｉｊ＝Ｘｉ（Ｚｊ）

【数４】ｋｊｉ＝Ｘｊ（Ｚｉ）

【数５】ｋｉｊ＝ｋｊｉ＝ｋ

【文献１】松本勉、今井秀樹、”第３の鍵共有方式”、１９８６年暗号と情報セキュリテイワークショップ講演論文集、１９８６年８月。

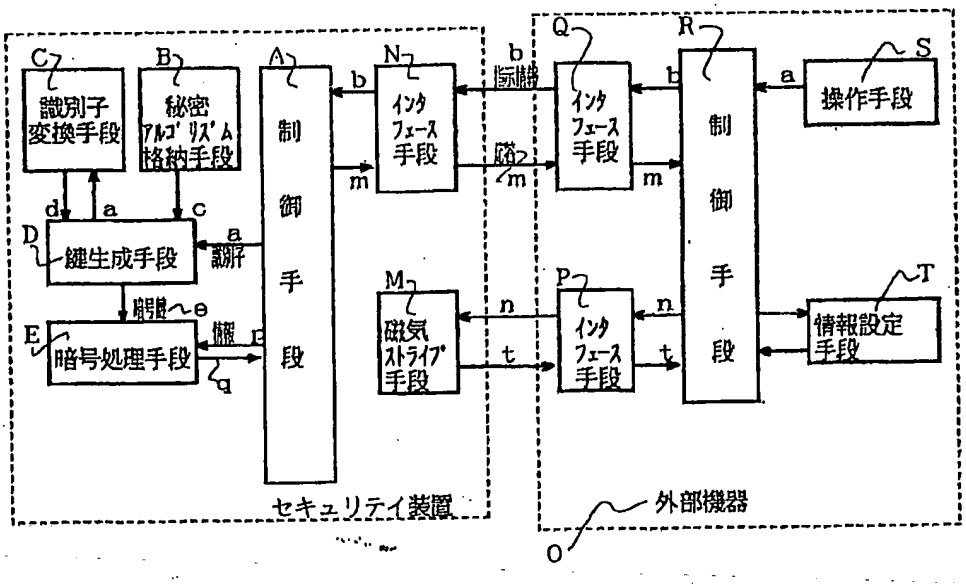
【文献２】松本勉、今井秀樹、”簡便な暗号鍵共有方式”、電気通信学会誌ＩＴ８６－５４、Ｐ－２９～３４、１９８６年９月。

【文献３】松本勉、今井秀樹、”キー プレデイストリビューション システムの一方式”（”ＫＥＹ ＰＲＥＤＩＳＴＲＩＢＵＳＩＯＮ ＳＹＳＴＥＭ ＢＡＳＥＤ ＯＮ ＬＩＮＥＡＲ ＡＬＧＥＢＲＡ”）、第９回情報理論とその応用シンポジウム、ＳＩＴＡ’８６，１９８６年１０月。

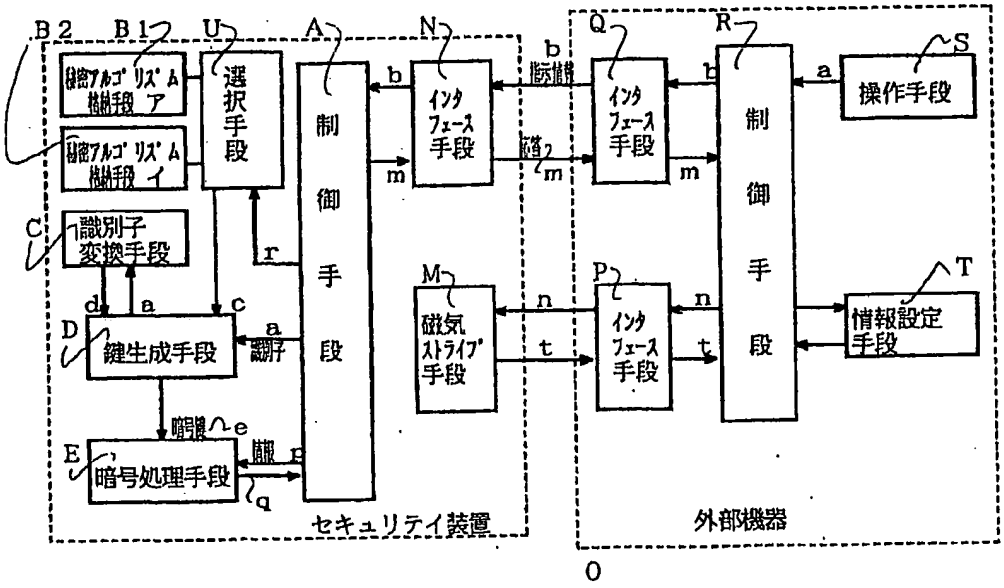
【文献４】松本勉、今井秀樹、”アプライング ザ キー プレデイストリビューション システム トウ エレクトリニク メイル アンド シグネチュア”，情報理論とその応用シンポジウム、ＳＩＴＡ’８７，１９８７年１１月。（Ｔｓｕｔｏｍｕ ＭＡＴＳＵＭＯＴＯ ａｎｄ，Ｈｉｄｅｋｉ ＩＭＡＩ，”Ａｐｐｌｙｉｎｇ ｔｈｅ Ｐｒｅｄｉｓｔｒｉｂｕｔｉｏｎ Ｓｙｓｔｅｍｔｏ Ｅｌｅｃｔｒｏｎｉｃ Ｍａｉｌｓ ａｎｄ Ｓｉｇｎａｔｕｒｅｓ”，ＳＩＴＡ’８７，ＮＯＶ．，１９８７．）

【文献５】松本勉、今井秀樹、”パフォーマンス オブ リニア スキーム フォア ザ キー プレデイストリビューション システム”、ＩＥＩＣＥ情報セキュリテイ技術報告、５月２０日号、１９８９年。（Ｔｓｕｔｏｍｕ ＭＡＴＳＵＭＯＴＯ ａｎｄ，Ｈｉｄｅｋｉ ＩＭＡＩ，”Ｐｅｒｆｏｒｍａｎｃｅ ｏｆ ｌｉｎｅａｒ ｓｃｈｅｍｅｓ ｆｏｒｔｈｅ Ｋｅｙ Ｐｒｅｄｉｓｔｒｉｂｕｔｉｏｎ Ｓｙｓｔｅｍ”，ＩＥＩＣＥ Ｔｅｃｈｎｉｃａｌ ｒｅｐｏｒｔ ｏｎ Ｉｎｆｏｒｍａｔｉｏｎ Ｓｅｃｕｒｉｔｙ，Ｍａｙ ２０，１９８８．）

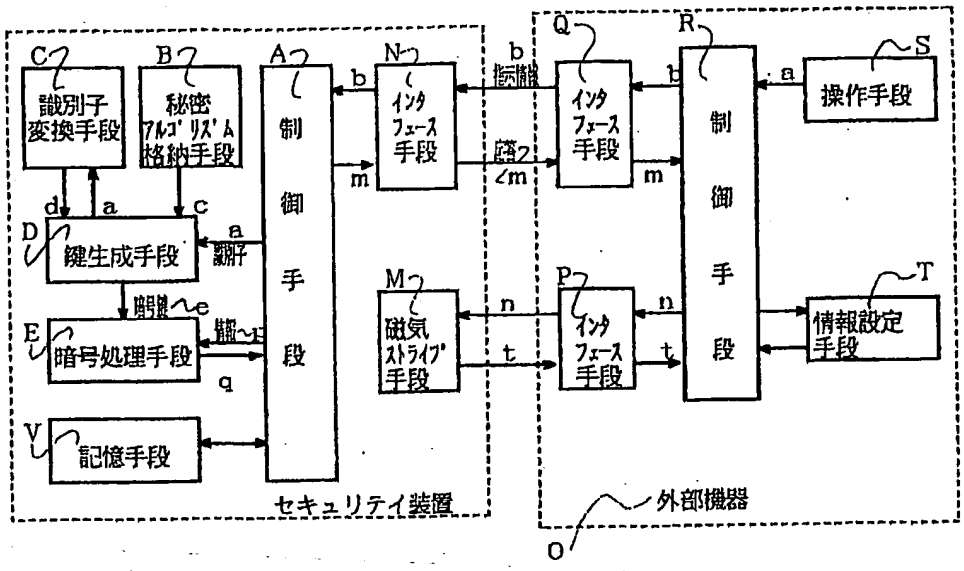
【図1】


C
識別子変換手段
B
秘密アルゴリズム格納手段
A
制御手段
N
インタフェース手段
b
転送情報
Q
インタフェース手段
R
制御手段
S
操作手段
d
a
c
D
鍵生成手段
a
選択
M
磁気ストライプ手段
P
インタフェース手段
T
情報設定手段
暗号鍵
e
E
暗号処理手段
情報
p
q
n
t
セキュリティ装置
外部機器
O

【図2】


B2
B1
U
A
N
Q
R
S
秘密アルゴリズム格納手段 ア
秘密アルゴリズム格納手段 イ
選択手段
制御手段
インタフェース手段
操作手段
C
識別子変換手段
r
d
a
c
D
鍵生成手段
M
磁気ストライプ手段
P
T
情報設定手段
暗号鍵
e
E
暗号処理手段
情報
p
q
セキュリティ装置
外部機器
O

【図3】


C
識別子
変換手段
B
秘密
ｱﾙｺﾞﾘｽﾞﾑ
格納手段
A
制御手段
N
インタフェース手段
b
指示識
m
d
a
c
D
鍵生成手段
a
識別子
鍵
e
E
暗号処理手段
識
q
V
記憶手段
セキュリティ装置
Q
インタフェース手段
R
制御手段
S
操作手段
T
情報設定手段
M
磁気ストライプ手段
P
インタフェース手段
n
t
外部機器
O